

**VIRTUAL PRIVATE NETWORK:
ARCHITECTURE AND IMPLEMENTATIONS**

A thesis submitted to the graduate school in partial
fulfillment of the requirements for the degree
Master of Science (Information Technology)
Universiti Utara Malaysia

by
KHAIRUL NAJMY HAJI ABDUL RANI

© Khairul Najmy Haji Abdul Rani, 2000. All rights reserved



Sekolah Siswazah
(Graduate School)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certification of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

KHAIRUL NAJMY HAJI ABDUL RANI

calon untuk Ijazah
(candidate for the degree of) Sarjana Sains (Teknologi Maklumat)

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

VIRTUAL PRIVATE NETWORK : ARCHITECTURE AND IMPLEMENTATIONS

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan,
dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory
knowledge of the field is covered by the project paper).

Nama Penyelia
(Name of Supervisor) : En. Helmi Mohamed Hussain

Tandatangan
(Signature) : Helmi Hussain

Tarikh
(Date) : 22 OKTOBER 2000

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or, in their absence, by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

**Dean of Graduate School
Universiti Utara Malaysia
06010 Sintok
Kedah Darulaman
Malaysia**

ABSTRAK

Revolusi ekonomi berasaskan rangkaian telah mengubah **cara** manusia menjalankan aktiviti-aktiviti pemiagaan. Di dalam **hal ini**, keperluan-keperluan komunikasi terkini diperlukan untuk menjadikan pemiagaan lebih berdaya saing. Sebagai contoh, sesetengah staf **kini mungkin** bekerja di dalam **bangunan** yang berlainan atau **malahan** negeri yang berlainan dengan **pengurus** mereka. Jadi satu jaringan meliputi kawasan **luas** diperlukan **bagi** memudahkan kedua-dua pihak **pengurus** dan staf-staf **tersebut** untuk berkomunikasi **walaupun** pada jarak yang berjauhan. Contoh **seterusnya**, menjalankan **kerjasama** atau perkongsian **pintar** di antara **syarikat-syarikat** adalah merupakan satu **strategi pemiagaan** yang sangat penting, terutamanya dalam menghadapi tekanan saingan pemiagaan. Oleh yang **demikian**, satu rangkaian komunikasi yang selamat diperlukan **bagi** menghubungkan **syarikat-syarikat** yang terlibat di dalam proses kerjasama atau perkongsian **pintar** pemiagaan itu. Salah satu **penyelesai** untuk Rangkaian Kawasan Luas (WAN) yang digunakan **bagi** memenuhi keperluan-keperluan komunikasi yang kompleks **tertera** di atas, dikenali sebagai **Virtual Private Network (VPN)**. VPN adalah satu teknologi terkini yang menggunakan Internet sebagai tulang belakang rangkaian yang **utama**.

Secara amnya, VPN telah dikatakan lebih fleksibel, **efektif**, dan **efisien** dalam menjalankan pemiagaan berbanding dengan teknologi-teknologi WAN yang **lain**. Terdapat dua fungsi utama yang membuatkan VPN menjadi **salah satu penyelesai alternatif** WAN pada masa **kini**: Penekanan *privacy* di dalam **melakukan pertukaran** data yang sensitif melalui cara yang lebih murah berbanding dengan penyelesai-penyelesai WAN tradisional, dan **juga** perlindungan keselamatan yang **sangat** baik terhadap **aset-aset maklumat** yang dihantar melalui infrastruktur Internet.

Adalah menjadi satu kebaikan untuk memahami teknologi VPN secara **terperinci** sebelum ianya digunakan. Di dalam projek ini, terdapat kajian mengenai VPN dari segi **latarbelakang** pembangunan, konfigurasi, jenis-jenis **aplikasi**, **ciri-ciri** penyelesai (keselamatan), kerangka rekabentuk, kebaikan dan keburukan jika dibandingkan dengan teknologi-teknologi saingan, *Quality of Service (QoS)* dan *Service Level of Agreements (SLAs)*, IO-langkah berguna untuk membina infrastruktur VPN, dan penggunaan VPN di dunia nyata. Diharapkan, laporan projek ini dapat menjadi sebagai satu rujukan atau petunjuk yang berguna terutamanya kepada mereka yang berminat di dalam merekabentuk, membangun, dan mengimplementasikan teknologi VPN.

Pada kenyataannya, VPN adalah merupakan satu teknologi baru dan boleh diperkembangkan lagi. Terdapat beberapa kelemahan di dalam senibinanya dan ciri-ciri penyelesaiannya, di mana ianya perlu dikembangkan lagi. Projek ini memfokuskan teknologi VPN berbanding dengan teknologi-teknologi saingannya di dalam menyediakan penyelesaian terbaik di dalam rangkaian *Enterprise* sesebuah organisasi.

ABSTRACT

The revolution of the networked-centric economy has transformed the way of people carrying out business activities. In this case, the business needs new kind of communication requirements in order to be more competitive. For instance, some corporate staffs are no longer work in the same building or even in the same country with their managers. Therefore a wide area link is needed to communicate with these staffs working in the remote branches or in the fields. Another example, alliances and partnerships among enterprises have become as crucial strategies that need to be regulated by many industries to cater the pressures from business competitors. Therefore, a secure communication solution is needed to link all the joined enterprises. One of the latest emerged Wide Area Network (WAN) solutions used to fulfill all the complex communication requirements is **known** as **Virtual Private Network** (VPN), which use the Internet as the main backbone.

In general, VPN has been claimed to be more flexible, effective and efficient compared to other WAN technologies. Two essential functions that make VPN as one of the best alternative WAN solutions currently: Privacy for interchange of sensitive data in a cheaper way compared to traditional WAN solutions, and Remarkable security protection of information assets transmitted over the Internet infrastructure.

It is good to understand the VPN technology in details before starting to implement it. In this thesis, there will be a study on VPN in terms of its progression backgrounds? configurations, application types, solution (security) features, design framework, pros and cons with respect to other competitor technologies, Quality of Service (QoS) and Service Level Agreements (SLAs), **useful** lo-point plan infrastructure building, real world implementation. **Hopefully** this thesis can be as a useful reference or guidance for those who are really interested in designing, developing, and implementing the VPN technology.

In reality, VPN is an immature and upgradable technology. There are certain loopholes in its architectures and solution features that can be enhanced. This project will focus on VPN's technology compared to other WAN solutions in providing the best solution for the organization's enterprise network.

ACKNOWLEDGEMENT

Firstly, *Syukur Alhamdulillah* and great thanks to ALLAH TA'ALA for giving me opportunities in terms of healthy mind and body, patience, as well as sufficient time and energy to finish up this project. I would also like to show great appreciation to Mr. Helmi Mohamed Hussain who was my project supervisor. Though he was busy, he still could spend time with me to give a lot of useful guidance and constructive ideas in making this project become so successful and have research values. Not forgotten, I would like to give high gratitude to Mr. Abdul Razak Jusoh, an Information System officer from the UUM Computer Center Department for providing me with some useful information and layouts of the existing UUM Integrated Sintok Local Area Network (ISLAN) and Mrs. Fauzuniah Pangil, a Lecturer from the UUM School of Management for helping me out in preparing this project report.. Finally, I would like to express high gratefulness to my wife Mrs. Alawiyah Hj. Abd. Wahab, my only daughter Nurul Najihah Khairul Najmy, and all of my other family members, relatives and friends for keep supporting me to finish up this project and through it to complete my MSc.IT program course work successfully. All co-operations, supports and guidance that you guys gave me are greatly appreciated and may ALLAH TA'ALA bless all of you.

Thanks and best regards.

Yours sincerely,

KHAIRUL NAJMY HJ. ABDUL RANI (81303)

MSc.IT (UUM)

OCTOBER 2000

TABLE OF CONTENTS

	Page:
PERMISSION TO USE.....	i
ABSTRAK (BAHASA MALAYSIA).....	ii
ABSTRACT (ENGLISH LANGUAGE).....	iv
ACKNOWLEDGEMENT.....	v
TABLE OF CONTENTS.....	vi
LIST OF TABLES.....	x
LIST OF FIGURES.....	xi

CHAPTER 1: INTRODUCTION

1.1	Today's Corporate Requirements for High-Performance and Secure WAN Solution.....	1
1.2	Problem Statements.....	2
1.3	Objectives of Project.....	3
1.4	Scopes and Limitations of Project.....	3
1.5	Significance of Project.....	4
1.6	Methodology.....	4

CHAPTER 2: INTRODUCING VPN

2.1	Definition of VPN.....	8
2.2	Overview of VPN.....	9
2.3	Histories and Timeline (Evolution) of VPN.....	11
2.3.1	Introduction of the Internet.....	11
2.3.2	Timeline (Evolution) of VPN.....	12
2.3.3	The First Remote Access VPN.....	14
2.3.4	The First Tunnel Protocol.....	15
2.3.5	The Emergence of Layer-2 Forwarding (L2F).....	15
2.3.6	The Emergence of Point-to-Point Tunneling Protocol (PPTP).....	16
2.3.7	The Emergence of Layer-2 Tunneling Protocol (L2TP).....	16
2.3.8	The Emergence of Internet Protocol Security (IPSec).....	17
2.4	Market Trends of VPN.....	17
2.5	Key Players of VPN.....	21
2.5.1	Cisco Systems.....	21
2.5.2	Nortel Networks.....	23
2.5.3	IBM Networking Divisions.....	24
2.5.4	Microsoft Corporation.....	24
2.5.5	Enterasys Incorporated.....	24
2.5.6	Nokia Incorporated.....	25
2.6	Environment Suitable for VPN.....	27

TABLE OF CONTENTS

	Page:
CHAPTER 3: CONFIGURATION OF VPN	
3.1 Untrusted Private Network.....	28
3.2 Trusted Private Network.....	29
3.3 Corporate-to-the Internet.....	30
3.4 De-Militarized Zone (DMZ).....	31
3.5 Behind an Existing Firewall.....	32
3.6 Additional Firewall and Tunnel Functionality.....	33
3.7 Adding a VPN Gateway to an Existing Firewall Infrastructure.....	33
3.8 Internal Applications.....	34
CHAPTER 4: APPLICATIONS OF VPN	
4.1 Extranet Application.....	36
4.2 Remote Access Application.....	37
4.3 Intranet (Site-to-Site) Application.....	38
4.4 Enterprise Application (E-VPN).....	39
4.5 Firewall Application.....	41
4.6 Internal Application.....	41
CHAPTER 5: CORE COMPONENTS FOR A ROBUST IMPLEMENTATION OF VPN	
5.1 Attributes to Ensure Robust IP-VPN Service Provisioning and Operations.....	42
CHAPTER 6: SOLUTION FEATURES OF VPN	
6.1 Internet-Firewall.....	44
6.2 Encryption/Decryption.....	50
6.3 Authentications and Access Protocol.....	57
6.4 Encapsulation and Tunneling Protocols.....	59
6.4.1 Internet Protocol Security protocol (IPSec).....	60
6.4.2 Point-to-Point Tunneling Protocol (PPTP).....	66
6.4.3 Layer-2 Tunneling Protocol (L2TP).....	69
6.4.4 Layer-2 Forwarding protocol (L2F).....	73
6.4.5 Generic Routing Encapsulation protocol (GRE).....	77
CHAPTER 7: A REFERENCE OF FRAMEWORK DESIGN FOR VPN	
7.1 Design Methodology.....	79
7.2 Scenario Scope.....	80

TABLE OF CONTENTS

	Page:
7.3 Conceptual Design.....	80
7.3.1 Global Conceptual Design.....	80
7.3.2 Local Conceptual Design.....	80
7.4 Logical Design.....	81
7.4.1 Local Logical Remote Access VPN Design.....	81
7.4.2 Local Logical Intranet and Local Logical Extranet Design...	82
7.4.3 Global Logical Design.....	83
7.5 Physical Design.....	84
7.5.1 Software-Based VPN.....	85
7.5.2 Hardware-Based VPN.....	88
7.5.3 Carrier-Based (Service Provider) VPN.....	88
 CHAPTER 8: COMPARISON BETWEEN COMPETITOR TECHNOLOGIES AND VPN	
8.1 VPN versus Frame Relay.....	89
8.2 VPN versus Dedicated Point-to-Point (Leased Line).....	92
8.3 VPN versus X.25.....	95
8.4 VPN versus ISDN.....	100
8.5 VPN versus DSL.....	104
 CHAPTER 9: QUALITY OF SERVICE (QoS) & SERVICE LEVEL AGREEMENT (SLA) FOR VPN	
9.1 Introducing QoS.....	109
9.2 Packet Classification.....	110
9.3 Bandwidth Management.....	111
9.4 Traffic Shaping.....	113
9.5 Congestion Avoidance.....	113
9.6 Enhanced Traffic Management.....	115
9.5 SLA Checklists and Future Perspective.....	116
 CHAPTER 10: A TEN-POINT PLAN FOR BUILDING A VPN	
10.1 Assess Your Connectivity Requirements.....	118
10.2 Implement or Update the Corporate Security Policy.....	118
10.3 Determine a Backup Plan.....	119
10.4 Determine the Best Product or Service Solution.....	120
10.5 Test Proposed Solution.....	120
10.6 Size the System.....	120
10.7 Pick the Location for the VPN Equipment.....	121
10.8 Reconfigure Other Network Devices.....	121
10.9 Install and Configure the VPN.....	121

TABLE OF CONTENTS

	Page:
10.10 Monitor and Manage the VPN.....	122
 CHAPTER 11: CASE STUDY	
11.1 VPN Solutions Implemented in the Real World.....	123
11.2 VPN Implementation in the Black & Veatch Corporation.....	123
11.3 VPN Implementation in the Forum Corporation.....	125
11.4 VPN Proposed for UUM Main Campus and Branch Campuses Nationwide.....	127
11.5 The Design of the Proposed VPN for UUM.....	127
11.6 The Configuration of the Proposed VPN for UUM.....	135
11.7 Alternative Hardware and Software Components for the Proposed VPN.....	137
11.8 Method Used for the Proposed VPN Connectivity.....	138
 CHAPTER 12: CONCLUSIONS	
	139
 CHAPTER 13: REFERENCES	
	144

LIST OF TABLES

Table:	Description:	Page:
Table 1	VPN Market Phases and Characteristics.....	14
Table 2	Leased Line and Internet-Based VPN Operating Cost Comparison.....	94

LIST OF FIGURES

Figure:	Description:	Page:
Figure 1.1	Diagram of Methodology Relationships.....	5
Figure 2.1	Virtual Private Network.....	8
Figure 2.2	Overall Structure of a Secure VPN.....	10
Figure 2.3	Tunneling Process.....	11
Figure 2.4	Internet-Based VPN.....	12
Figure 2.5	Current Market Profile of VPN.....	19
Figure 2.6	Type and Protocol of VPN in Market.....	20
Figure 2.7	Nokia IP Network Application Platform.....	26
Figure 3.1	LAN-to-LAN Connection for an Untrusted Private Networks.....	29
Figure 3.2	LAN-to-LAN Connection for a Trusted Private Networks.....	30
Figure 3.3	VPN Client vs. the Internet User.....	31
Figure 3.4	Secure Corporate Network and DMZ.....	32
Figure 3.5	VPN Gateway and Existing Third-Party Firewall.....	32
Figure 3.6	VPN Gateway and 3 rd Party Firewall with Network Paths.....	33
Figure 3.7	VPN Gateway Added to an Existing Firewall Infrastructure.....	34
Figure 3.8	VPN Gateway Added to Create a Secure LAN within a Company.....	35
Figure 4.1	Extranet VPN.....	36
Figure 4.2	Remote Access VPN.....	37
Figure 4.3	Intranet VPN.....	38
Figure 4.4	Enterprise VPN (E-VPN).....	40
Figure 4.5	Cisco's 5-Point E-VPN Strategy.....	40
Figure 6.1	Screening Router Forming a Security Perimeter.....	46
Figure 6.2	Circuit-Level Gateway Operation.....	47
Figure 6.3	Application-Level Gateway Operation.....	48
Figure 6.4	Cisco Secure PIX Firewall in a Network.....	49
Figure 6.5	Plaintext versus Ciphertext.....	50
Figure 6.6	The Caesar Cipher.....	51
Figure 6.7	Key for Vigenere's Cipher.....	52
Figure 6.8	Transposition Cipher's Two Dimensional Array.....	53
Figure 6.9	An IPSec Scenario.....	61
Figure 6.10	An IPSec AH.....	62
Figure 6.11	An IPSec ESP Format.....	63
Figure 6.12	Transport Mode vs. Tunnel Mode Encryption.....	65
Figure 6.13	Typical L2TP Network Topology.....	70
Figure 6.14	L2TP Structure.....	71
Figure 6.15	Tunneling PPP during the L2TP Session.....	72
Figure 6.16	Generic Internet with the PSTN and ISDN Accesses.....	73
Figure 6.17	Logging on to Access VPNs.....	74
Figure 6.18	Protocol Negotiation Events between Access VPN Devices.....	75
Figure 6.19	L2F Tunnel Authentication Process.....	76

LIST OF FIGURES

Figure:	Description:	Page:
Figure 6.20	Three-Way CHAP Authentication Process.....	76
Figure 6.21	GRE Tunnel Architecture for E-VPN.....	78
Figure 7.1	Local Logical Remote Access VPN Design.....	82
Figure 7.2	Local Logical Intranet and Local Logical Extranet VPN Design...	82
Figure 7.3	Global Logical Design.....	84
Figure 8.1	Frame Relay Components.....	90
Figure 8.2	Dedicated Point-to-Point (Leased Line) Connection Between Sites.....	92
Figure 8.3	The X.25 Model.....	96
Figure 8.4	The X.25 Frame Formats.....	97
Figure 8.5	Analog vs. ISDN Connections.....	100
Figure 8.6	ISDN BRI Service Configuration.....	101
Figure 8.7	ISDN PRI Service Configuration.....	102
Figure 8.8	ADSL Network Structure.....	105
Figure 9.1	Packet Classification at Network Ingress.....	111
Figure 9.2	ToS Field in the IP Packet Header.....	112
Figure 9.3	Weighted Fair Queuing.....	113
Figure 9.4	Generic Traffic Shaping.....	113
Figure 9.5	Weighted Random Early Detection (WRED).....	114
Figure 9.6	Global TCP Synchronization.....	114
Figure 9.7	MPLS Operations.....	115
Figure 11.1	ISLAN Design.....	130
Figure 11.2	UUM Main Campus Proposed VPN Configuration.....	135
Figure 11.3	UUM Branch Campus Proposed VPN Configuration.....	136

CHAPTER 1

Introduction

1.1 Today's Corporate Requirements for High-Performance and Secure Wide Area Network (WAN) Solutions

The emergence of digital communication systems particularly computer networks has changed significantly the way people practice businesses during this information age. Formerly, computer networks were considered merely a convenient method of sharing resources or sending simple messages [38]. Today, computer networks have become a key component of a corporation's strategic assets, and a driving force in transformation of Information Technology (IT) from a back-office tool to a marketplace weapon, where there should be a continuous evaluation of information network's ability to fully support corporate goals and missions [38].

Two important things have to be emphasized simultaneously by businesses in evaluating information network's ability. Firstly, the network should have the capability to support a broader variety of communications among a wider range of sites. This is due to current employees extensive demand to access the resources of their corporate intranets as they take to the road, telecommute, or dial in from customer sites. Furthermore, business partners, outside consultants and vendors sometimes are required to join together in the extranets to share or exchange business information so that a joint project can successfully be done for long-term strategic benefits [40].

Secondly, the infrastructure of the networks should be designed, built and managed at a low cost. In this case, the characteristics demanded by current business environment in the development of "virtual offices" and "virtual project teams" are more typically found in public, rather than private data networks [38]. Thus, it is no doubt to say that the exponential growth of the Internet and the emergence of Web-based intranets have encouraged corporations to evaluate the low cost, ubiquitous and highly scalable Internet as a potential replacement for private networks as the primary medium for corporate data communications [38].

The contents of
the thesis is for
internal user
only

CHAPTER 13

REFERENCES

1. Airamo, Joona. "Virtual Private Networks", 1997.
http://www.tem/hut.fi/Opinnot/Tik-110.501/1997/virtual_private_networks
2. Beyda, William J. Data Communications: From Basic to Broadband. 2nd ed. Prentice Hall International, 1996.
3. Chae, Lee. "Lesson 123: Virtual Private Networks", 1998.
<http://www.networkmagazine.com/magazine/tutorial/9810tut.htm>
4. Cooper, Frederic J, Chris Goggans, John K. Halvey, Larry Hughes, Lisa Morgan, Karanjit Siyan, William Stallings and Peter Stephenson. Implementing Internet Security. 1st ed. Indianapolis: New Riders Publishing, 1995.
5. DaSilva, Luiz A. "Frame Relay Presentation", 1999.
<http://www.ee.vt.edu/~ee46141d/fr.pdf>
6. "Delivering New World Virtual Private Networks with MPLS". A Cisco Systems Incorporated White Paper.
http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/tech/mppls_wi.htm
7. "Encryption". A Novell Corporation White Paper
<http://www.novell.com/corp/legal/encrypt.html>
8. "Enterasys's Virtual Private Network". An Enterasys Incorporated Handout.
<http://www.enterasys.com/vpn/>
9. Ferrell, Tom. "Virtual Private Networking Is Real Technology-Now".
<http://www.vpdn.com/content/vpnbackground/whitepapers/compatible.html>
10. "Frame Relay". A Pulsecom Incorporated White Paper.
<http://www.pulsecom.com/framewp.htm>
11. "Leased Lines". A Galaxy Internet Services Incorporated White Paper, 1999.
<http://www.gis.net/business/leasedlines.html>
12. Gele, Brian J. "Digital Subscriber Line (DSL) Services: A New Telecommunications Alternative?", 1997.
<http://www.instantweb.com/m/mahesh/4453/DSL.HTML>
13. Herscovitz, Eli. "Secure Virtual Private Networks: The Future of Data Communications", 1998.
<http://www.vpdn.com/content/vpnbackground/whitepapers/RADGUARD.html>

14. Hughes, Larry J. Actually Useful Internet Security Techniques. 1st ed. Indianapolis: New Riders Publishing, 1995.
15. "Introduction: Quality of Service Overview". A Cisco Systems Inc. White Paper. www.cisco.com/univercd/cc/td/doc/product/software/ios/20/12cgr/qos_c/qcintro.htm
16. "IPSec". A Cisco Systems Incorporated White Paper. http://www.cisco.com/warp/public/cc/cisco/mkt/security/encryp/tech/ipsec_wp.htm
17. "ISDN: The Evolution of Digital Communication". An Eicon Inc. White Paper. <http://www.eicon.com/ISDN/whtpap1.htm>
18. "LanRover VPN Gateway Site Planning Guide". <http://www.shiva.com/pdf/vpnsite.pdf>
19. "Managed IPsec VPNs: Building Virtual Private Network". A Cisco Systems Incorporated White Paper. www.cisco.com/warp/public/779/servpro/services/vpn/VPN_Managed_IPSec_TSD.pdf
20. "Networks Go Virtual". A 3Com Corporation White Paper. http://www.3com.com/news/vpn_jp.html
21. "Overview of Access VPNs and Tunneling Technologies". A Cisco Systems Incorporated White Paper. http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/vpn_soln/vpdnover.htm
22. "Quality of Service for Virtual Private Networks". A Cisco Systems Incorporated White Paper. http://www.cisco.com/warp/public/cc/sol/mkt/ent/vpne/tech/qsvpn_wp.htm
23. Ranum, Marcus J. and Matt Curtin. "Internet Firewalls Frequently Asked Questions", 1998. <http://www.clark.net/pub/mjr/pubs/fwfaq>
24. "Redefining the Virtual Private Network (VPN)". A Checkpoint Inc. White Paper. <http://www.checkpoint.com/products/vpn1/vpndef.html>
25. "Reference Guide: A Primer for Implementing a Cisco Virtual Private Network". A Cisco Systems Incorporated White Paper. http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm
26. "Remote Network Access Using Digital Subscriber Line Technology". A Flowpoint Corporation White Paper, 1999. <http://www.flowpoint.com/tlc/whitepapers/wp-rna/>

27. Salamone, S. "VPN White Paper: The Basic VPN Implementation Calls for a Tunnel Trip", 1998.
<http://www.internetwk.com/VPN/paper-5.htm>
28. Scott, C. "Why Build a Virtual Private Network". A Microsoft Corporation White Paper, 2000.
<http://www.microsoft.com/technet/network/vpnch1.asp>
29. Semeria, Chuck. "Internet Firewalls and Security: A Technology Overview". A 3Com Corporation White Paper, 1996.
<http://www.3com.com/nsc/500619.html>
30. Shay, William A. Understanding Data Communications and Networks. 2nd ed. Pacific Grove: Brooks/Cole Publishing, 1999.
31. Sheldon, Tom. "General Firewall White Paper", 1996.
<http://www.ntresearch.com/firewall.htm>
32. Stallings, William. "IP Security". A Cisco Systems Inc. White Paper, 2000.
http://www.cisco.com/warp/public/759/ipj_3_1_ip.html
33. Taylor, Laura and Bradley Hecht. "VPNs are Hot, but Where are They?", 1999.
http://idm.internet.com/articles/199911/ft_11_16_99a.html
34. "The Bargain Hunter's Guide to Global Networking – Virtual Private Networks", A CIO Online Article.
http://www.cio.com/archive/040199_vpn.html
35. "Troubleshooting X.25 Connections". A Cisco Systems Inc. White Paper.
http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1919.htm
36. "Understanding PIX Firewall". A Cisco Systems Inc. White Paper, 2000.
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v52/config/intro.htm
37. "Understanding Point-to-Point Tunneling Protocol (PPTP)". Microsoft Corporation White Paper, 1997.
http://msdn.microsoft.com/library/backgrnd/html/Understanding_PPTP.htm
38. "VPLink Technology". A VPNet Corporation White Paper, 1998.
<http://www.vpnet.com/products/vplink.html>
39. "What Is... a firewall (a definition)", 2000.
<http://whatis.com/firewall.htm>

40. "Web ProForum Tutorial: VPNs". A Nortel Networks Inc. White Paper, 2000.
<http://www.webproforum.com/vpn/index.html>
41. "Welcome to Mistral Internet – Services (Leased Line)". A Mistral Incorporated White Paper.
<http://www.mistral-uk.net/lline.htm>
42. "White Paper: Security Issues for Enterprise VPNs". A Cisco Systems Incorporated White Paper.
http://www.cisco.com/warp/public/cc/sol/mkt/ent/vpne/tech/sevpn_wp.htm
43. "Wide Area Networking: A User's Guide". An Intel Incorporated White Paper.
http://www.intel.com/network/white_papers/wide_area.htm
44. "Virtual Private Network".
<http://www.whatis.com/vpn.htm>
45. "VPN: High Availability to Insure Continuous Internet Connectivity". A Nokia Incorporated White Paper.
<http://www.nokia.com/securitysolutions/network/availability.html>
46. "VPN and IPSec Supported Standards". A Cisco Systems Inc. White Paper.
www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v52/ipsec/intro.htm
47. "VPN: Managed Firewall Services with Nokia Security Solutions". A Nokia Incorporated White Paper.
<http://www.nokia.com/securitysolutions/network/managedfirewall.html>
48. "X.25 Packet Switched Networks". A Sangoma Incorporated White Paper.
<http://www.sangoma.com/x25.htm>
49. Ybarra, Dano. "DSL White Paper". A Flowpoint Corporation White Paper, 1998.
http://www.flowpoint.com/tlc/whitepapers/flowpoint/wp_dslmk.html
50. "56/64 Kbps Leased Lines".
<http://www.mot.com/MIMS/ISG/projects/technology/ll.html>.